UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,882	07/08/2003	Philip Michael Hawkes	030441	9835

23696 7590 02/02/2009

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
02/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/615,882	**Applicant(s)** HAWKES ET AL.	
	Examiner MICHAEL J. SIMITOSKI	**Art Unit** 2434	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 22 January 2009 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☒ They raise the issue of new matter (see NOTE below);
   (c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *64-86*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Michael J Simitoski/
Primary Examiner, Art Unit 2434

Continuation of 3. NOTE: At least claim 66 raises the issue of new matter and requires further consideration as the limitation was not previuosly presented.

Continuation of 11. does NOT place the application in condition for allowance because:

Applicant's response (p. 9, ¶2) argues that the Hawkes publication fails to disclose "wherein the content provider encrypts a broadcast access key with each of the unique public keys to authorize a terminal having the secure processing unit securely storing a corresponding unique private key to receive the encrypted multimedia content". Repeating the statement made in the rejection, the Examiner agrees with this statement as the RK of Hawkes is disclosed as a symmetric key, where the same data value (RK) that is used to encrypt the BAK (to form what Hawkes calls BAKI), is also used to decrypt the BAK.

Applicant's response (p. 9, ¶3) argues that the key encrypting key (KEK) in Ahonen is similar to the BAK in Hawkes because the KEK of Ahonen is unique to the subscriber and the subscriber's KEK is unicast to the subscriber, where Hawkes' BAK is common to a group of subscribers and the common BAK is encrypted by the user unique registration key RK. First, it is noted that Applicant has pointed to the background of Ahonen, rather than the description of the invention. More importantly, the motivations behind both Hawkes and Ahonen are identical – to provide encrypted content to a user and to provide the keys used for the encryption of that content to the user. Both Hawkes and Ahonen utilize a content key (Hawkes, SK; Ahonen, TEK). Both Hawkes and Ahonen utilize a key that encrypts the content key (i.e. a key encrypting key) (Hawkes, BAK; Ahonen, KEK). Both Hawkes and Ahonen utilize a key known to the terminal that is used to decrypt the (received, encrypted) key encrypting key (Hawkes, RK; Ahonen, terminal private key). For clarity, Hawkes uses the structure (CONTENT)SK, (SK)BAK, (BAK)RK, where Ahonen uses (CONTENT)TEK, (TEK)KEK, KEK(terminal private key). Applicant's response notes that the BAK of Hawkes is a key used by multiple subscribers, whereas the KEK of Ahonen is a key used by only one subscriber and uses this as rationale that Hawkes cannot be modified such that instead of a symmetric RK, a public/private key pair is used as the top-level key, gaining the advantages shown in Ahonen (particularly the advantage that, in Hawkes, the RK must at some point be assigned to the terminal and to the content provider in a secure manner not transmitted publicly, whereas in Ahonen, the private key could be generated within the subscriber terminal and the public portion simply transmitted publicly to any and all recipients, such as a content provider). However, the Examiner submits that this distinction does not preclude this use. The sharing of an intermediate key in the hierarchy of Hawkes' invention does not reduce the benefits gained from the Ahonen public key approach because an intermediate key is used individually in Ahonen. Further, if the "group" of subscribers in Hawkes comprises a single subscriber, the keys (Hawkes' BAK and Ahonen's KEK) have exactly the same use. In light of the parallel uses of the keys described above, and the benefit gained from the modification suggested, the rejection is maintained.

Applicant's response (p. 10, ¶1) argues Hawkes' brief description of public-key cryptography. The cited portion of Hawkes is a general description of public-key cryptography and lists both the benefits and shortcomings of both public-key methods and secret key methods. This paragraph is a general statement and does not teach away from using public key cryptography. Any generalization that there are both benefits and shortcomings of a particular technology would not teach away from using that technology. There has been no evidence cited that the modification of Hawkes' invention in the manner described would destroy Hawkes' invention. Further, while not relied upon in the rejection, it should be noted that a skilled artisan understands the benefits of public key cryptography versus symmetric key cryptography and the suggested modification is well within the realm of one having such ordinary skill at the time the invention was made.

Applicant's amendments to the claims objected to based on informalities overcome the previous claim objections.